WHAT IS CLAIMED IS:

1. A method of handling client state information, said method comprising:

receiving, at a first computer system, a first request from a second computer system, wherein the first request is received over a computer network;

identifying access control data pertaining to the second computer system;

creating an encrypted value based upon the access control data; and

storing, on the second computer system, a state management data structure that includes an access control identifier and the encrypted value.

2. The method of claim 1 further comprising:

authenticating a user of the second computer system; and

caching, on the first computer system, security attributes of the authenticated user that are too sensitive to be included in the state management data structure, wherein the cached security attributes are indexed by the encrypted value and wherein cached security attributes are adapted to re-establish a security context of the authenticated user.

3. The method of claim 1 wherein the access control identifier is selected from the group consisting of

the access control data and a unique identifier used by the first computer system to map to the access control data stored on an authentication server.

4. The method of claim 1 wherein at least one field included in the access control data is selected from the group consisting of: a domain, a maximum age, a path, a port, an authentication strength value, an authenticating server identifier, and an access control privilege identifier.

5. The method of claim 1 wherein the creation of the encrypted value further comprises:

hashing the access control data using a hashing algorithm, the hashing resulting in a hash value; and

encrypting the hash value.

6. The method of claim 1 further comprising:

storing the encrypted value at the first computer system in response to receiving the first request;

receiving a second request from the second computer system;

retrieving the state management data structure from the second computer system, the retrieving performed in conjunction with the reception of the second request; and

comparing the encrypted value included in the retrieved state management data structure with the encrypted value stored at the first computer system.

7. The method of claim 6 further comprising:

re-establishing an authenticated user's security context by using the encrypted value as a key to retrieve the access control data cached on the first computer system.

8. The method of claim 1 further comprising:

authenticating a user of the second computer system, wherein the identifying, creating, and storing are performed in response to successfully authenticating the user.

9. The method of claim 8 further comprising:

determining that the third computer system does not have access to the authentication data;

retrieving the authentication data from an authentication server in response to the determination; and

storing the retrieved authentication data on a cache associated with the third computer system.

10. The method of claim 1 further comprising:

receiving, at the first computer system, a second request from the second computer system;

retrieving the state management data structure from the second computer system, the retrieving performed in conjunction with the reception of the second request;

determining that the retrieved state management data structure is stale based on a timestamp included in the state management data structure; and

authenticating a user of the second computer system in response to the determination.

11. An first information handling system comprising:

one or more processors;

a memory accessible by the processors;

a network interface connecting the information handling system to a computer network;

a tool for handling client state information, the tool including software effective to:

receive, at the first information handling system, a first request from a second information handling system, wherein the first request is received over a computer network;

identify access control data pertaining to the second information handling system;

create an encrypted value based upon the access control data; and

store, on the second information handling system, a state management data structure that includes an access control identifier and the encrypted value.

12. The information handling system of claim 11 further comprising software effective to:

authenticate a user of the second information handling system; and

cache, on the first information handling system, security attributes of the authenticated user that are too sensitive to be included in the state management data structure, wherein the cached security attributes are indexed by the encrypted value and wherein cached security attributes are adapted to re-establish a security context of the authenticated user.

13. The information handling system of claim 11 wherein the access control identifier is selected from the group consisting of the access control data and a unique identifier used by the first information handling system to map to the access control data stored on an authentication server.

14. The information handling system of claim 11 wherein at least one field included in the access control data is selected from the group consisting of: a domain, a maximum age, a path, a port, an authentication strength value, an authenticating server identifier, and an access control privilege identifier.

15. The information handling system of claim 11 wherein the creation of the encrypted value further comprises software effective to:

hash the access control data using a hashing algorithm, the hashing resulting in a hash value; and

encrypt the hash value.

16. The information handling system of claim 11 further comprising software effective to:

store the encrypted value at the first information handling system in response to receiving the first request;

receive a second request from the second information handling system;

retrieve the state management data structure from the second information handling system, the retrieval performed in conjunction with the reception of the second request; and

compare the encrypted value included in the retrieved state management data structure with the encrypted value stored at the first information handling system.

17. The information handling system of claim 16 further comprising software effective to:

re-establish an authenticated user's security context by using the encrypted value as a key to retrieve the access control data cached on the first information handling system.

18. The information handling system of claim 11 further comprising software effective to:

authenticate a user of the second information handling system, wherein the identifying, creating, and storing are performed in response to successfully authenticating the user.

19. The information handling system of claim 18 further comprising software effective to:

determine that a third information handling system does not have access to the authentication data;

retrieve the authentication data from an authentication server in response to the determination; and

store the retrieved authentication data on a cache associated with the third information handling system.

20. The information handling system of claim 11 further comprising software effective to:

receive, at the first information handling system, a second request from the second information handling system;

retrieve the state management data structure from the second information handling system, the retrieving performed in conjunction with the reception of the second request;

determine that the retrieved state management data structure is stale based on a timestamp included in the state management data structure; and

authenticate a user of the second information handling system in response to the determination.

21. A computer program product stored on a computer operable media for handling client state data, said computer program product comprising:

means for receiving, at a first computer system, a first request from a second computer system, wherein the first request is received over a computer network;

means for identifying access control data pertaining to the second computer system;

means for creating an encrypted value based upon the access control data; and

means for storing, on the second computer system, a state management data structure that includes an access control identifier and the encrypted value.

22. The computer program product of claim 21 further comprising:

means for authenticating a user of the second computer system; and

means for caching, on the first computer system, security attributes of the authenticated user that are too sensitive to be included in the state management data structure, wherein the cached security attributes are indexed by the encrypted value and wherein cached security attributes are adapted to re-establish a security context of the authenticated user.

23. The computer program product of claim 21 wherein the access control identifier is selected from the group consisting of the access control data and a unique identifier used by the first computer system to map to the access control data stored on an authentication server.

24. The computer program product of claim 21 wherein at least one field included in the access control data is selected from the group consisting of: a domain, a maximum age, a path, a port, an authentication strength value, an authenticating server identifier, and an access control privilege identifier.

25. The computer program product of claim 21 wherein the means for creating the encrypted value further comprises:

means for hashing the access control data using a hashing algorithm, the hashing resulting in a hash value; and

means for encrypting the hash value.

26. The computer program product of claim 21 further comprising:

means for storing the encrypted value at the first computer system in response to receiving the first request;

means for receiving a second request from the second computer system;

means for retrieving the state management data structure from the second computer system, the means for retrieving performed in conjunction with the reception of the second request; and means for comparing the encrypted value included in the retrieved state management data structure with the encrypted value stored at the first computer system.

27. The computer program product of claim 26 further comprising:

means for re-establishing an authenticated user's security context by using the encrypted value as a key to retrieve the access control data cached on the first computer system.

28. The computer program product of claim 21 further comprising:

means for authenticating a user of the second computer system, wherein the identifying, creating, and storing are performed in response to successfully authenticating the user.

29. The computer program product of claim 28 further comprising:

means for determining that the third computer system does not have access to the authentication data;

means for retrieving the authentication data from an authentication server in response to the determination; and

means for storing the retrieved authentication data on a cache associated with the third computer system.

30. The computer program product of claim 21 further comprising:

means for receiving, at the first computer system, a second request from the second computer system;

means for retrieving the state management data structure from the second computer system, the means for retrieving performed in conjunction with the reception of the second request;

means for determining that the retrieved state management data structure is stale based on a timestamp included in the state management data structure; and

means for authenticating a user of the second computer system in response to the determination.